Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 30.10.2026 13:36:03
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

*Высшая школа интеллектуальных систем и кибертехнологий*

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# Б1.В.ДВ.02.2 «Компьютерная вирусология»

Направление подготовки:

**10.03.01 «Информационная безопасность»**

Направленность (профиль):

**«Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)»**

Квалификация выпускника: **бакалавр**

Тольятти 2025

Рабочая программа дисциплины «Компьютерная вирусология» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования – бакалавриат по направлению подготовки 10.03.01 «Информационная безопасность», утвержденным приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 г. № 1427.

Составители:

| | |
|---|---|
| старший преподаватель | Ю.С. Мунирова |
| (ученая степень, ученое звание) | (ФИО) |

РПД обсуждена на заседании ученого совета Высшей школы интеллектуальных систем и кибертехнологий

«23» _05_ 2025_ г., протокол № _10_

| | | |
|---|---|---|
| Директор | к.э.н., доцент | О.А. Филиппова |
| | (уч.степень, уч.звание) | (ФИО) |

## 1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

### 1.1. Цель освоения дисциплины

Целями освоения дисциплины являются:

– формирование у обучающихся системных теоретических знаний о принципах функционирования, классификации и жизненном цикле компьютерных вирусов и иного вредоносного программного обеспечения;

– формирование умения организовывать защиту информации ограниченного доступа от воздействия вредоносного программного обеспечения в соответствии с нормативными правовыми актами и методическими документами;

– формирование навыков применения программных, программно-аппаратных и технических средств защиты информации автоматизированных систем от вредоносного программного обеспечения.

– формирование у обучающихся общепрофессиональных компетенций *в области использования информационно-коммуникационных технологий*

– *углубление уровня освоения обучающимися* профессиональных компетенций, необходимых для решения задач профессиональной деятельности.

### 1.2. Перечень планируемых результатов обучения по дисциплине

| **Код и наименование компетенции** | **Код и наименование индикатора достижения компетенции** | **Планируемые результаты обучения по дисциплине** | **Основание (ПС)** *для профессиональных компетенций |
|---|---|---|---|
| ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю | ИОПК-6.1. Применяет технологии, методы и средства защиты информации ограниченного доступа | Знает:<br>– принципы функционирования и классификацию компьютерных вирусов и иного вредоносного программного обеспечения; требования нормативных и методических документов ФСТЭК России в области антивирусной защиты<br><br>Умеет:<br>– применять технологии, методы и средства защиты информации ограниченного доступа от воздействия вредоносного программного обеспечения<br><br>Владеет:<br>– навыками организации защиты информации ограниченного доступа от вредоносного программного | |

| | | | |
|---|---|---|---|
| | | обеспечения в соответствии с действующими нормативными требованиями | |
| ПК-4. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах | ИПК-4.1. Применяет программные, программно-аппаратные и технические средства защиты информации автоматизированных систем, в том числе криптографические методы, алгоритмы и протоколы<br>ИПК-4.2. Осуществляет конфигурирование параметров программных, программно-аппаратных и технических средств защиты информации автоматизированных систем | Знает:<br>– принципы работы и архитектуру антивирусных средств защиты автоматизированных систем; методы анализа вредоносного программного кода<br><br>Умеет:<br>– осуществлять конфигурирование параметров антивирусных средств защиты автоматизированных систем<br><br>Владеет:<br>– навыками применения средств анализа и нейтрализации вредоносного программного обеспечения | 06.033 Специалист по защите информации в автоматизированных системах |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы и является элективной дисциплиной, углубляющей освоение профиля (Дисциплины по выбору).

# 3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

## 3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ представлено в таблице.

| Виды учебных занятий и работы обучающихся | Трудоемкость, час |
|---|---|
| **Общая трудоемкость дисциплины, час** | **108** |
| **Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:** | **86/52** |
| **занятия лекционного типа** (лекции) | 40/20 |
| **занятия семинарского типа** (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия) | 46/32 |
| **Самостоятельная работа, всего** | **22/52** |
| **Контроль (часы на зачет)** | -/4 |
| **Промежуточная аттестация** | **Зачет** |

Примечание: *-/- объем часов соответственно для очной и очно-заочной формы обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

### 3.2. Содержание дисциплины, структурированное по темам

| Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций | Наименование разделов, тем | Виды учебной работы | | | Формы текущего контроля (наименование оценочного средства) |
|---|---|---|---|---|---|
| | | Контактная работа | | Самостоятельная работа, час | |
| | | Лекции, час | Практические занятия, час | | |
| ОПК-6<br>ИОПК-6.1 | **ТЕМА 1. ИСТОРИЯ И КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ**<br>Основное содержание:<br>1. История развития компьютерных вирусов и вредоносного программного обеспечения.<br>2. Классификация компьютерных вирусов по среде обитания, способу заражения, деструктивным возможностям.<br>3. Нормативные и методические документы, регламентирующие защиту от вредоносного программного обеспечения. | 3/4 | | | Устный опрос |
| | Практическое занятие № 1. Классификация образцов вредоносного программного обеспечения | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 6/4 | |
| ОПК-6<br>ИОПК-6.1 | **ТЕМА 2. ЖИЗНЕННЫЙ ЦИКЛ КОМПЬЮТЕРНОГО ВИРУСА**<br>Основное содержание:<br>1. Жизненный цикл компьютерного вируса: фазы заражения, инкубации, активации, проявления.<br>2. Механизмы внедрения вируса в систему.<br>3. Способы маскировки и сокрытия присутствия вируса в системе. | 3/4 | | | |

| | | | | | |
|---|---|---|---|---|---|
| | Практическое занятие № 2. Анализ жизненного цикла типового образца вредоносного ПО | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 7/4 | |
| ОПК-6<br>ИОПК-6.1 | **ТЕМА 3. ФАЙЛОВЫЕ И ЗАГРУЗОЧНЫЕ ВИРУСЫ**<br>Основное содержание:<br>1. Файловые вирусы: принципы функционирования и заражения исполняемых файлов.<br>2. Загрузочные вирусы и буткиты: принципы функционирования.<br>3. Методы обнаружения файловых и загрузочных вирусов. | 2/4 | | | Доклад/сообщение |
| | Практическое занятие № 3. Исследование методов обнаружения файловых вирусов | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 6/4 | |
| ПК-4<br>ИПК-4.1 | **ТЕМА 4. МАКРОВИРУСЫ, СКРИПТОВЫЕ ВИРУСЫ И СЕТЕВЫЕ ЧЕРВИ**<br>Основное содержание:<br>1. Макровирусы и скриптовые вирусы: особенности распространения.<br>2. Сетевые черви: механизмы распространения и заражения.<br>3. Методы противодействия распространению сетевых червей. | 2/4 | | | |
| | Практическое занятие № 4. Анализ механизмов распространения сетевого червя | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 7/4 | |

| | | | | | |
|---|---|---|---|---|---|
| ПК-4<br>ИПК-4.1 | **ТЕМА 5. ТРОЯНСКИЕ ПРОГРАММЫ И ПРОГРАММЫ-ШИФРОВАЛЬЩИКИ**<br>Основное содержание:<br>1. Троянские программы и бэкдоры: назначение и принципы функционирования.<br>2. Программы-шифровальщики (ransomware): принципы функционирования и методы противодействия.<br>3. Меры реагирования на инциденты, связанные с программами-шифровальщиками. | 3/4 | | | |
| | Практическое занятие № 5. Анализ поведения троянской программы в изолированной среде | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 6/4 | |
| ПК-4<br>ИПК-4.1,<br>ИПК-4.2 | **ТЕМА 6. МЕТОДЫ АНАЛИЗА ВРЕДОНОСНОГО ПРОГРАММНОГО КОДА**<br>Основное содержание:<br>1. Методы статического анализа вредоносного программного кода.<br>2. Методы динамического анализа вредоносного программного кода (запуск в изолированной среде).<br>3. Технологии обнаружения неизвестных ранее образцов вредоносного ПО (эвристический, поведенческий анализ). | 3/4 | | | Устный опрос / тестирование |
| | Практическое занятие № 6. Проведение статического и динамического анализа образца вредоносного ПО | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 7/4 | |
| ОПК-6 | **ТЕМА 7.** | 2/4 | | | |

| | | | | | |
|---|---|---|---|---|---|
| ИОПК-6.1 | **ПОЛИМОРФНЫЕ И МЕТАМОРФНЫЕ ВИРУСЫ**<br>Основное содержание:<br>1. Полиморфные и метаморфные вирусы: методы противодействия обнаружению.<br>2. Технологии обфускации вредоносного программного кода.<br>3. Методы обнаружения полиморфных вирусов сигнатурными и эвристическими средствами. | | | | |
| | Практическое занятие № 7. Исследование методов обхода антивирусной защиты полиморфными вирусами | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 6/4 | |
| ПК-4<br>ИПК-4.2 | **ТЕМА 8. АРХИТЕКТУРА АНТИВИРУСНЫХ СРЕДСТВ И ОРГАНИЗАЦИЯ ЛАБОРАТОРНОГО АНАЛИЗА**<br>Основное содержание:<br>1. Архитектура и принципы работы антивирусных средств защиты.<br>2. Конфигурирование параметров антивирусных средств защиты автоматизированных систем.<br>3. Организация лабораторного анализа образцов вредоносного программного обеспечения. | 2/4 | | | Практическое задание / тестирование |
| | Практическое занятие № 8. Конфигурирование антивирусного средства защиты и организация лабораторного анализа образца ПО | | 4/4 | | Практическое задание |
| | Самостоятельная работа | | | 7/4 | |
| | **ИТОГО** | **40/20** | **46/32** | **22/52** | |

Примечание: *-/- объем часов соответственно для очной и очно-заочной формы обучения*

# 4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

## 4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых университетом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий**:

- балльно-рейтинговая технология оценивания;
- электронное обучение;
- проблемное обучение;
- разбор конкретных ситуаций (кейс-метод);
- информационные технологии, применяемые в электронной информационно-образовательной среде университета.

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

## 4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины, обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

Отдельные вопросы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим (лабораторным) занятиям, выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

## 4.3. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа / на практических занятиях

Практические (лабораторные) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы дисциплины. Основной формой проведения занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение практических задач и выполнение заданий на персональном компьютере.

Практические (лабораторные) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и практических навыков по учебному материалу дисциплины;

– подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Занятия организуются, в том числе, в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

**4.4. Методические указания по самостоятельной работе обучающихся**

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине.

Самостоятельная работа студентов включает:

– изучение учебной литературы и нормативных документов по курсу;
– подготовку к практическим (лабораторным) занятиям;
– решение практических ситуаций и задач;
– работу с ресурсами информационно-телекоммуникационной сети «Интернет»;
– подготовку к тестированию по темам курса;
– подготовку к промежуточной аттестации по курсу.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

# 5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

**5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

Вся литература, включенная в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объеме не менее 0,25 экземпляров на одного обучающегося.

**Основная литература:**

1. Мельников, В. П. Информационная безопасность и защита информации : учебное пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков. – Москва : Академия. – Текст : электронный.

2. Бирюков, А. А. Информационная безопасность: защита и нападение : учебное пособие / А. А. Бирюков. – Москва : ДМК Пресс. – Текст : электронный.

3. Казарин, О. В. Безопасность программного обеспечения компьютерных систем : монография / О. В. Казарин. – Москва : МГУЛ. – Текст : электронный.

**Дополнительная литература:**

4. Скляров, Д. В. Искусство защиты и взлома информации / Д. В. Скляров. – Санкт-Петербург : БХВ-Петербург. – Текст : непосредственный.

5. Фленов, М. Е. Компьютер глазами хакера / М. Е. Фленов. – Санкт-Петербург : БХВ-Петербург. – Текст : непосредственный.

6. Учебно-методическое пособие по дисциплине «Компьютерная вирусология» : для студентов направления подготовки 10.03.01 «Информационная безопасность» / Поволж. гос. ун-т сервиса (ФГБОУ ВО «ПВГУС») ; сост.: Ю. С. Мунирова. – Тольятти : ПВГУС. – Текст : электронный.

**5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы**

1. Официальный сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России) : сайт. – URL: https://fstec.ru – Текст : электронный.

2. Банк данных угроз безопасности информации ФСТЭК России (БДУ) : сайт. – URL: https://bdu.fstec.ru – Текст : электронный.

3. Национальный координационный центр по компьютерным инцидентам (НКЦКИ) : сайт. – URL: https://safe-surf.ru – Текст : электронный.

4. eLIBRARY.RU : научная электронная библиотека : сайт. – URL: https://elibrary.ru – Текст : электронный.

5. Электронная библиотечная система Поволжского государственного университета сервиса : сайт / ФГБОУ ВО «ПВГУС». – Тольятти. – URL: http://elib.tolgas.ru – Режим доступа: для авториз. пользователей. – Текст : электронный.

**5.3. Программное обеспечение**

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

| № п/п | Наименование | Условия доступа |
|---|---|---|
| 1 | Антивирусное программное обеспечение отечественного производства | из внутренней сети университета (лицензионный договор) |
| 2 | Изолированная среда выполнения (песочница) для анализа вредоносного ПО | из компьютерных классов университета (свободно распространяемое программное обеспечение) |

| | | |
|---|---|---|
| 3 | Инструментальные средства статического и динамического анализа кода | из компьютерных классов университета (свободно распространяемое программное обеспечение) |
| 4 | КонсультантПлюс | из внутренней сети университета (лицензионный договор) |
| 5 | СДО MOODLE | из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор) |

## 6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

**Занятия лекционного типа.** Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования – проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

**Занятия семинарского типа.** Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования – проектор, экран, компьютер/ноутбук).

**Промежуточная аттестация.** Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета, и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

**Самостоятельная работа.** Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются: компьютерные классы университета; библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети «Интернет».

**Электронная информационно-образовательная среда университета (ЭИОС).** Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории университета, так и вне ее.

ЭИОС университета обеспечивает: доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей),

программах практик; формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

## 7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла; в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации;

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

## 8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

### 8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100

**Шкала оценки результатов освоения дисциплины, сформированности результатов обучения**

| **Форма проведения промежуточной аттестации** | **Шкалы оценки уровня сформированности результатов обучения** | | **Шкала оценки уровня освоения дисциплины** | | |
|---|---|---|---|---|---|
| | Уровневая шкала оценки компетенций | 100 бальная шкала, % | 100 бальная шкала, % | 5-балльная шкала, дифференцированная оценка/балл | недифференцированная оценка |
| *зачет* | допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 | не зачтено |
| | пороговый | 61-85,9 | 61-69,9 | «удовлетворительно» / 3 | зачтено |
| | | | 70-85,9 | «хорошо» / 4 | зачтено |
| | повышенный | 86-100 | 86-100 | «отлично» / 5 | зачтено |

*По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.*

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество*

**Формы текущего контроля успеваемости**

| Формы текущего контроля | Количество контрольных точек | Баллов за 1 точку | Макс. балл |
|---|---|---|---|
| Устный опрос/доклад сообщение | 3 | 8 | 24 |
| Решение практических заданий | 8 | 7 | 56 |
| Тестирование по темам курса | 2 | 10 | 20 |
| **Итого** | | | **100 баллов** |

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

### 8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

#### 8.2.1. Типовые задания к практическим занятиям

1. Классификация образцов вредоносного программного обеспечения.
2. Анализ жизненного цикла типового образца вредоносного ПО.
3. Исследование методов обнаружения файловых вирусов.
4. Анализ механизмов распространения сетевого червя.
5. Анализ поведения троянской программы в изолированной среде.
6. Проведение статического и динамического анализа образца вредоносного ПО.
7. Исследование методов обхода антивирусной защиты полиморфными вирусами.
8. Конфигурирование антивирусного средства защиты и организация лабораторного анализа образца ПО.

#### 8.2.2. Типовые тестовые задания для текущего контроля

*Правильные варианты ответов выделены жирным шрифтом.*

**1. Программа, способная создавать свои копии и внедрять их в файлы, загрузочные секторы дисков без ведома пользователя, называется:**

**А) компьютерным вирусом**

Б) операционной системой

В) архиватором

Г) компилятором

**2. Вирус, заражающий загрузочные секторы дисков, называется:**

А) файловым вирусом

**Б) загрузочным вирусом**

В) макровирусом

Г) скриптовым вирусом

**3. Вредоносная программа, самостоятельно распространяющаяся по компьютерной сети без внедрения в другие файлы, называется:**

**А) сетевым червем**

Б) файловым вирусом

В) макровирусом

Г) буткитом

**4. Вредоносная программа, шифрующая файлы пользователя с целью получения выкупа, называется:**

**А) программой-шифровальщиком (ransomware)**

Б) антивирусом

В) файловым менеджером

Г) архиватором

**5. Вирус, изменяющий свой программный код при каждом новом заражении для затруднения обнаружения, называется:**

А) файловым вирусом

**Б) полиморфным вирусом**

В) загрузочным вирусом

Г) макровирусом

**6. Метод анализа вредоносного кода, предполагающий его запуск в изолированной среде для наблюдения за поведением, называется:**

А) статическим анализом

**Б) динамическим анализом**

В) регрессионным тестированием

Г) нагрузочным тестированием

**7. Программа, предоставляющая злоумышленнику скрытый удаленный доступ к зараженной системе, называется:**

**А) бэкдором**

Б) браузером

В) драйвером

Г) компилятором

**8. Изолированная программная среда, предназначенная для безопасного запуска и анализа подозрительных файлов, называется:**

**А) песочницей (sandbox)**

Б) файрволом

В) прокси-сервером

Г) маршрутизатором

**Темы докладов/сообщений**

1. История развития компьютерных вирусов и вредоносного программного обеспечения.

2. Классификация компьютерных вирусов по среде обитания, способу заражения, деструктивным возможностям.

3. Нормативные и методические документы, регламентирующие защиту от вредоносного программного обеспечения.

4. Жизненный цикл компьютерного вируса: фазы заражения, инкубации, активации, проявления

**Вопросы для устного опроса**

1. Сетевые черви: механизмы распространения и заражения.

2. Троянские программы и бэкдоры: назначение и принципы функционирования.

3. Программы-шифровальщики (ransomware): принципы функционирования и методы противодействия.

4. Методы статического анализа вредоносного программного кода.

5. Методы динамического анализа вредоносного программного кода (запуск в изолированной среде).

### 8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: зачет (по результатам накопительного рейтинга или в форме компьютерного тестирования).

Устно-письменная форма по вопросам к зачету предполагается, как правило, для сдачи академической задолженности.

**Перечень вопросов для подготовки к зачету**

**ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю**

1. История развития компьютерных вирусов и вредоносного программного обеспечения.
2. Классификация компьютерных вирусов по среде обитания, способу заражения, деструктивным возможностям.
3. Нормативные и методические документы, регламентирующие защиту от вредоносного программного обеспечения.
4. Жизненный цикл компьютерного вируса: фазы заражения, инкубации, активации, проявления.
5. Файловые вирусы: принципы функционирования и заражения исполняемых файлов.
6. Загрузочные вирусы и буткиты: принципы функционирования.
7. Макровирусы и скриптовые вирусы: особенности распространения.
8. Организация защиты информации ограниченного доступа от вредоносного программного обеспечения.
9. Полиморфные и метаморфные вирусы: методы противодействия обнаружению.
10. Отчетность и документирование инцидентов, связанных с вредоносным программным обеспечением.

**ПК-4. Способен выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных и технических средств защиты информации автоматизированных системах**

1. Сетевые черви: механизмы распространения и заражения.
2. Троянские программы и бэкдоры: назначение и принципы функционирования.
3. Программы-шифровальщики (ransomware): принципы функционирования и методы противодействия.
4. Методы статического анализа вредоносного программного кода.
5. Методы динамического анализа вредоносного программного кода (запуск в изолированной среде).
6. Архитектура и принципы работы антивирусных средств защиты.

7. Конфигурирование параметров антивирусных средств защиты автоматизированных систем.

8. Методы нейтрализации и удаления вредоносного программного обеспечения.

9. Технологии обнаружения неизвестных ранее образцов вредоносного ПО (эвристический, поведенческий анализ).

10. Организация лабораторного анализа образцов вредоносного программного обеспечения.